

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10133953 A**

(43) Date of publication of application: 22 . 05 . 98

(51) Int. Cl

**G06F 12/14**  
**G06K 17/00**
(21) Application number: **08302554**

(22) Date of filing: 28 . 10 . 96

(71) Applicant: **TOKIMEC INC**
 (72) Inventor: **KYOMASU TAKAFUMI**  
**TERUYAMA KATSUYUKI**  
**ATSUMI YOSHIO**

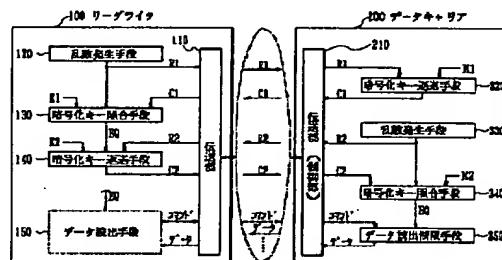
## (54) DATA SECRECY DEVICE

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To protect memory data more securely against illegal use by interception by replacing the initiative side and answer side of a communication with each other by secrecy reset data is ciphered and multiplied.

**SOLUTION:** When a 1st random number is generated by a 1st random number generating means 120, sent from one communication device 10, and received by the other communication device 200, a 1st ciphering key sending-back means 320 ciphers 1st secrecy reset data with the 1st random number and sends it back to the communication device 100 from the communication device 200 and a 1st ciphering key matching means 130 matches it against a 1st ciphered secrecy reset data. According to this matching result, it is decided whether or not memory data can be sent and received. Prior to the transmission and reception of the memory data, the other communication device 200 takes the initiative to communicate with the communication device 100 as an answer side, and then 2nd secrecy data is confirmed.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-133953

(43) 公開日 平成10年(1998) 5月22日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 12/14

G 0 6 K 17/00

識別記号

3 2 0

F I

G 0 6 F 12/14

G 0 6 K 17/00

3 2 0 C

3 2 0 B

F

S

審査請求 未請求 請求項の数 3 F D (全 9 頁)

(21) 出願番号

特願平8-302554

(22) 出願日

平成 8 年 (1996) 10 月 28 日

(71) 出願人 000003388

株式会社トキメック

東京都大田区南蒲田 2 丁目 16 番 46 号

(72) 発明者 京増 貴文

東京都大田区南蒲田 2 丁目 16 番 46 号 株式  
会社トキメック内

(72) 発明者 照山 勝幸

東京都大田区南蒲田 2 丁目 16 番 46 号 株式  
会社トキメック内

(72) 発明者 渥美 凱雄

東京都大田区南蒲田 2 丁目 16 番 46 号 株式  
会社トキメック内

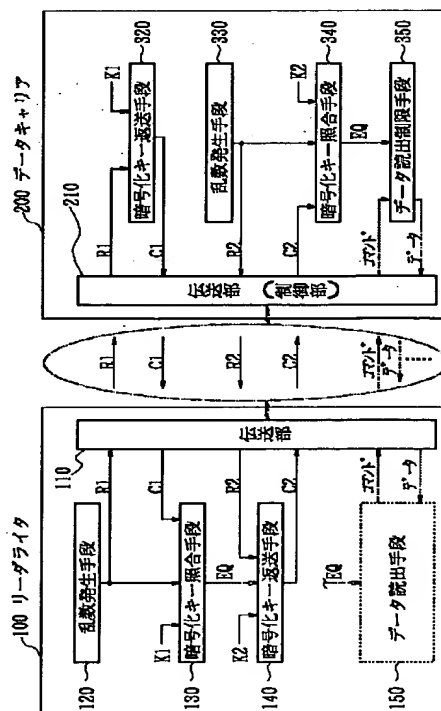
(74) 代理人 弁理士 佐藤 香

(54) 【発明の名称】 データ秘匿装置

(57) 【要約】

【課題】 通信を傍受しての不正使用から一層確実にメモリデータを保護する。

【解決手段】 電磁誘導結合でのメモリデータの送受信に先だって秘匿解除データの送受信および照合を行うデータ秘匿装置において、乱数 R1 を発生する第 1 乱数発生手段 120 と、受信した乱数 R1 で秘匿解除データ K1 を暗号化し暗号化済み秘匿解除データ C1 を返送する第 1 暗号化キー返送手段 320 と、受信した暗号化済み秘匿解除データ C1 について照合を行う第 1 暗号化キー照合手段 130 と、乱数 R2 を発生する第 2 乱数発生手段 330 と、受信した乱数 R2 で秘匿解除データ K2 を暗号化し暗号化済み秘匿解除データ C2 を返送する第 2 暗号化キー返送手段 140 と、受信した暗号化済み秘匿解除データ C2 について照合を行う第 2 暗号化キー照合手段 340 とを備え、暗号化キー照合手段 140, 340 の照合結果に基づいてメモリデータの送受信の可否を決する。



## 【特許請求の範囲】

【請求項1】電磁誘導結合に依り対をなしてメモリデータの送受信を行う一対のデータ通信装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ秘匿装置において、前記一対のデータ通信装置のうちの一方の通信装置に設けられ第1の乱数を発生する第1乱数発生手段と、前記一対のデータ通信装置のうちの他方の通信装置に設けられ前記一方の通信装置から受信した前記第1の乱数を用いて第1の秘匿解除データを暗号化しこの暗号化済み第1の秘匿解除データを前記一方の通信装置へ返送する第1暗号化キー返送手段と、前記一方の通信装置に設けられ前記他方の通信装置から受信した暗号化済み第1の秘匿解除データについて照合を行う第1暗号化キー照合手段と、前記他方の通信装置に設けられ第2の乱数を発生するとともにこれを前記第1の秘匿解除データの返送の後に送信する第2乱数発生手段と、前記一方の通信装置に設けられ前記他方の通信装置から受信した前記第2の乱数を用いて第2の秘匿解除データを暗号化しこの暗号化済み第2の秘匿解除データを前記他方の通信装置へ返送する第2暗号化キー返送手段と、前記他方の通信装置に設けられ前記一方の通信装置から受信した暗号化済み第2の秘匿解除データについて照合を行う第2暗号化キー照合手段とを備え、前記第1暗号化キー照合手段および前記第2暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータ秘匿装置。

【請求項2】電磁誘導結合によってデータ記憶体とメモリデータの送受信を行うデータアクセス装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータアクセス装置のデータ秘匿装置において、第1の乱数を発生する乱数発生手段と、前記データ記憶体から受信した暗号化済み第1の秘匿解除データについて照合を行う暗号化キー照合手段と、前記データ記憶体から受信した第2の乱数を用いて第2の秘匿解除データを暗号化しこの暗号化済み第2の秘匿解除データを前記データ記憶体へ返送する暗号化キー返送手段とを備え、前記暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータアクセス装置のデータ秘匿装置。

【請求項3】電磁誘導結合によってデータアクセス装置とメモリデータの送受信を行うデータ記憶体に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ記憶体のデータ秘匿装置において、前記データアクセス装置から受信した第1の乱数を用いて第1の秘匿解除データを暗号化しこの暗号化済み第1の秘匿解除データを前記データアクセス装置へ

返送する暗号化キー返送手段と、第2の乱数を発生するとともにこれを前記第1の秘匿解除データの返送の後に送信する乱数発生手段と、前記データアクセス装置から受信した暗号化済み第2の秘匿解除データについて照合を行う暗号化キー照合手段とを備え、前記暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータ記憶体のデータ秘匿装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、データ秘匿装置に関し、詳しくは、交番電磁界を用いた電磁誘導結合方式で通信するデータ通信装置に好適なデータ秘匿装置に関する。かかるデータ通信装置は、ICカードやデータキャリア等の（携帯形）データ記憶体と、これ又はこれらのうち通信可能なところまで近接したデータ記憶体に対し通信でアクセスして接触不要でデータの読み取り、書き込み、又は読み書きを行うリーダ等のデータアクセス装置とからなる。

【0002】そして、その内部回路は要部がIC化されていて解析・解読が設備・コスト面から困難なものとなっており、さらに、その通信方式では通信可能な地域的範囲が狭く且つ交信手順が非公開となっている。そのため、このデータ秘匿装置は、通信伝文を監視して得た情報に基づいてデータ記憶体のデータを書き換えようとする行為を主対象とすることで、一般の秘話装置よりも簡便な方式により、不正行為からデータ記憶体のデータを保護しようとするものである。

## 【0003】

【従来の技術】携帯形データ記憶体のデータに電磁誘導結合方式の通信でアクセスするデータアクセス装置の適用例として、図4(a)にブロック図で示したデータキャリアシステムが挙げられる。このシステムは、屋外や構築物あるいは車両・船舶等に据えて設置されるリーダライタ10（データアクセス装置）と、携帯に好適な小形サイズのデータキャリア20（データ記憶体）とからなるものである。極めて小規模なシステムではこの一対だけでも済むが、通常は、単一又は複数のリーダライタ10に対して多数のデータキャリア20が用いられ、リーダライタ10と通信可能な近距離にまで接近したデータキャリア20とが所定データの送受に要する短時間だけ動的に対を確立するようになっている。

【0004】リーダライタ10は、商用電力AC100Vの供給を受けて作動するものであり、マイクロプロセッサ14を有して、そのプログラム処理によって電力送給波やコマンドあるいは書き込みデータなどの送出を制御するようになっている。さらに、マイクロプロセッサ14の制御下で電力送給波等を交番電磁界としてデータキャリア20へ向けて出射するために、送信データ等で所定周波数の搬送波を変調する変調回路や変調済み送信

信号をパワー増幅する送信アンプ等からなる伝送部13と、送信信号を交番電磁界に変換するコイル11とを備えたものとなっている。

【0005】データキャリア20は、動作電力の供給をリーダライタ20から非接触で受けるために、交番電磁界による電力送給波等を受けるコイル21と、これで受けた電力送給波を整流・蓄電等して電源電圧を生成する整流回路22とを備えたものである。コイル21はコマンド等の受信コイルでもあり、コイル11からの交番電磁界によってコイル21に誘起した信号は、制御部23によって受理される。制御回路23は、コイル21の誘起信号を増幅する受信アンプや搬送波を除去する復調回路等からなる伝送部も兼ねたものとなっている。制御回路23は、受信したコマンドの内容に応じてチップセレクトCS、シフトクロックSK、受信データDI等の制御信号を生成し、これでメモリ24にアクセスしてデータの書き込み等を行うようになっている。

【0006】また、データキャリア20の伝送部には、送信処理のために変調回路や送信アンプも具備されており、コマンドの処理結果や、メモリ24からの読出データDOなどの送信信号は、制御回路23の制御に従って、変調回路によって搬送波に混合され、送信アンプによってパワー増幅されてから、コイル21を介して交番電磁界に変換・出射されるようになっている。

【0007】さらに、リーダライタ10の伝送部13には、データキャリア20の送信信号を受信するために、データキャリア20からの交番電磁界によってコイル11に誘起した誘起信号を増幅する受信アンプや、この信号から搬送波成分やノイズ成分を除去して復調する復調回路も具備されている。そして、マイクロプロセッサ14のプログラム処理によって、復調信号からデータを抽出したり、コマンド処理結果を確認する等の処理を行うようになっている。

【0008】かかるデータキャリアシステムでは、データキャリア20が電磁誘導結合による供給電力や小さな内蔵電池によって動作することから、データキャリア20のコイル21から出射される交番電磁界は微弱であり、通信可能な地域的範囲が狭い。そして、このようなデータキャリアシステムは、スキー場でのリフト搭乗券改札システムや乗合バス乗車券改札システムなどに応用される。この場合、各改札にリーダライタ10が設置され、多数のデータキャリア20はリストバンド状や切符状に形成されていて搭乗券・乗車券の代わりに各利用者によって所持される。さらに、各データキャリア20のメモリ24には、搭乗可能か否かの搭乗券情報や支払い済み料金の残額等がメモリデータとして保持されている。

【0009】そして、搭乗等の際に利用者が自己のデータキャリア20をリーダライタ10のコイル21に近づけてこれら一対のリーダライタ10及びデータキャリア

20が交信可能な状態になると、メモリデータの送受信が行われる。すなわち、リーダライタ10がデータキャリア20へ読出コマンド（リードコマンド）を送出し、これを受けてデータキャリア20がメモリ24から保持データを読み出してこれをリーダライタ10へ返送する。さらに、リーダライタ10はデータの内容をチェックし、データ更新の必要があると、リーダライタ10がデータキャリア20へ更新データと共に書込コマンドを送出し、これを受けてデータキャリア20がメモリ24の保持データを書き換えるのである。

【0010】従来のデータ秘匿装置は、このようなメモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことでメモリデータの送受信の可否を決するためにデータキャリアシステムに対して付加・内蔵されるものであり、特開平4-169990号公報記載のものが挙げられる。これは、リーダライタ10におけるマイクロプロセッサ14について、リードコマンドと一緒に所定値の秘匿解除データも送信するようにプログラム処理が改められるとともに（図4（b）参照）、データキャリア20については、秘匿解除データ（キー）の照合および送受信可否の判定を行う秘匿回路30と、秘匿回路30の判定結果に従ってメモリデータの読み出しを制限するために読出データDOの信号ラインに介挿され読出データDO以外の入力として秘匿回路30の判定結果の信号を受けるANDゲート41とが設けられたものである。

【0011】秘匿回路30は、受信データDIをシリアル入力としシフトクロックSKをタイミング信号とするシフトレジスタ31を有してこれにリーダライタ10からの受信秘匿解除データをロードする一方で、読出データDOをシリアル入力としシフトクロックSKをタイミング信号とするシフトレジスタ32を有してこれにメモリ24の所定アドレスから読み出した読出秘匿解除データ等をロードするとともに、シフトレジスタ31、32の平行出力を両入力としこれらがする一致しているか否かの一致出力EQを生成出力する比較回路33を有して両秘匿解除データの照合を行う。さらに、シフトクロックSKのカウント34によるカウント値CNTを状態遷移の基準信号とする順序回路35を有し、この順序回路35で一致出力EQを全ビットに亘って監視し、両秘匿解除データが完全に一致しているときだけ、データ読出の制限を解除する信号がANDゲート41に送出されるようになっている。

【0012】このように秘匿解除データをデータアクセス装置から送信しそれをデータ記憶体で照合することで比較的簡便に、秘匿解除データが知られない限り不正行為からデータ記憶体のデータが保護される。一般にデータキャリアシステムは内部回路がIC化されることに加えて通信可能な地域的範囲が狭く且つ交信手順も公開されないのが、第三者の秘匿解除データ取得は困難であ

10

20

30

40

50

る。

#### 【0013】

【発明が解決しようとする課題】しかしながら、このような従来のデータ秘匿装置では、秘匿解除データがそのまま通信伝文に含められている。このため、例えば秘匿解除データ取得のための通信伝文傍受等が困難とは言っても、何らかの方策によって通信伝文が一旦傍受等された場合まで想定すると、秘匿解除データの特定・抽出に対する保護が万全とはいえない。また、通信手順も常時交互になされるので推定・把握しやすいといえる。そこで、通信傍受等により通信伝文を監視して得た情報に基づいてデータ記憶体のデータを書き換えようとする行為に対しても、一般の秘話装置よりも簡便な方式で、データ記憶体のデータを秘匿して保護することが課題となる。

【0014】この発明は、このような課題を解決するためになされたものであり、通信を傍受しての不正使用から一層確実にメモリデータを保護するデータ秘匿装置を実現することを目的とする。

#### 【0015】

【課題を解決するための手段】このような課題を解決するためになされた本発明について、その構成および作用効果を以下に説明する。なお、図1の機能ブロック図の符号も併記する。

【0016】この解決手段のデータ秘匿装置は、(出願当初の請求項1に記載の如く)、(互いのコイルやアンテナ等の間に確立された)電磁誘導結合に依り(一時的な又は恒常的な)対をなして(メモリからの読出データ及びメモリへの書込データの何れか一方または双方の)メモリデータの送受信を行う一対のデータ通信装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ秘匿装置において、前記一対のデータ通信装置のうちの一方の通信装置(100)に設けられ、第1の乱数(R1)を発生する第1乱数発生手段(120)と、前記一対のデータ通信装置のうちの他方の通信装置(200)に設けられ、前記一方の通信装置(100)から受信した前記第1の乱数(R1)を用いて第1の秘匿解除データ(K1)を暗号化しこの暗号化済み第1の秘匿解除データ(C1)を前記一方の通信装置(100)へ返送する第1暗号化キー返送手段(320)と、前記一方の通信装置(100)に設けられ、前記他方の通信装置(200)から受信した暗号化済み第1の秘匿解除データ(C1)について(自己の保持する第1の秘匿解除データ(K1)との)照合を行う第1暗号化キー照合手段(130)と、前記他方の通信装置(200)に設けられ、第2の乱数(R2)を発生するとともに、これを前記第1の秘匿解除データ

(C1)の返送の後に(直ちに又は所定時間経過してから)送信する第2乱数発生手段(330)と、前記一方

の通信装置(100)に設けられ、前記他方の通信装置(200)から受信した前記第2の乱数(R2)を用いて第2の秘匿解除データ(K2)を暗号化しこの暗号化済み第2の秘匿解除データ(C2)を前記他方の通信装置(200)へ返送する第2暗号化キー返送手段(140)と、前記他方の通信装置(200)に設けられ、前記一方の通信装置(100)から受信した暗号化済み第2の秘匿解除データ(C2)について(自己の保持する第2の秘匿解除データ(K2)との)照合を行う第2暗号化キー照合手段(340)とを備え、前記第1暗号化キー照合手段(130)および前記第2暗号化キー照合手段(340)の照合結果に基づいて前記メモリデータの送受信の可否を決する(150, 350)ことを特徴とするものである。

【0017】このようなデータ秘匿装置にあっては、電磁誘導結合に依って対をなす一対のデータ通信装置間でメモリデータの送受信を行うに際し、データ改竄等の不正使用からメモリデータを保護するために、メモリデータの送受信に先だって秘匿解除データの送受信および照合が行われてメモリデータの送受信の可否が決定されるのであるが、保護強化のために特に秘匿解除データの送受信および照合が以下の如く行われる。

【0018】すなわち、第1乱数発生手段によって第1の乱数が生成され、これが一方の通信装置から送信されて他方の通信装置で受信されると、第1暗号化キー返送手段によって、第1の秘匿解除データがその第1の乱数で暗号化されて他方の通信装置から一方の通信装置へ返送され、さらに、第1暗号化キー照合手段によって、暗号化済み第1の秘匿解除データについて照合が行われる。そして、この照合結果に基づいてメモリデータの送受信の可否が決められる。

【0019】こうして、メモリデータの送受信に先だって一方の通信装置が主導し他方の通信装置が応答する通信が行われ、これに基づいて第1の秘匿解除データの確認が行われることから、第1の秘匿解除データを知らない者はメモリデータの送受信を始めることができないので、そのような者の不正使用からデータを秘匿し保護することができる。しかも、秘匿解除データが乱数で暗号化されて送受信の度に变化するので、送信伝文が傍受・監視されたとしても、秘匿解除データが特定・抽出されるおそれは、ほとんど無い。

【0020】また、引き続き、第2乱数発生手段によって第2の乱数が生成され、これが他方の通信装置から送信されて一方の通信装置で受信されると、第2暗号化キー返送手段によって、第2の秘匿解除データがその第2の乱数で暗号化されて一方の通信装置から他方の通信装置へ返送され、さらに、第2暗号化キー照合手段によって、暗号化済み第2の秘匿解除データについて照合が行われる。そして、この照合結果に基づいても、メモリデータの送受信の可否が決められる。

【0021】こうして、メモリデータの送受信に先だって先ほどとは逆に他方の通信装置が主導し一方の通信装置が応答する通信が行われ、これに基づいて第2の秘匿解除データの確認が行われることから、第2の秘匿解除データを知らない者はメモリデータの送受信を始めることができないので、そのような者の不正使用からデータを秘匿し保護することができる。しかも、秘匿解除データが乱数で暗号化されて送受信の度に変化するので、送信伝文が傍受・監視されたとしても、秘匿解除データが特定・抽出されるおそれは、ほとんど無い。

【0022】しかも、電磁誘導結合によるデータ通信装置の場合この電磁誘導結合を介して一方の通信装置から他方の通信装置へエネルギー供給がなされることが多い等のため一方の通信装置が主導し他方の通信装置が応答する手順でメモリデータの送受信が行われのが通例であるところ、逆に他方の通信装置が主導し一方の通信装置が応答する通信も組み合わせられている。このように主導する側が動的に入れ替わること及びそのタイミングを送信伝文の傍受・監視によって検知することは困難である。

【0023】これにより、単に秘匿解除データを暗号化および複数化したことを超えて、より確実に、不正使用からメモリデータが保護される。したがって、この発明によれば、従来よりも確実に不正使用からメモリデータを保護することができる。

#### 【0024】

【発明の実施の形態】このような解決手段で達成された本発明のデータ秘匿装置について、これを実施するための形態を説明する。

【0025】〔第1の実施の形態〕本発明の第1の実施形態は、上述した解決手段のデータ秘匿装置であって、前記一方の通信装置（100）が（、出願当初の請求項2に記載の如く）、上記の第1乱数発生手段（120）と第1暗号化キー照合手段（130）と第2暗号化キー返送手段（140）と前記第1暗号化キー照合手段（130）の照合結果に基づいて前記メモリデータの送受信の可否を決するデータ読出手段（150）とを備えたデータアクセス装置（データ読取装置、データ書込装置、データ読書装置）であり、前記他方の通信装置（200）が（、出願当初の請求項3に記載の如く）、上記の第1暗号化キー返送手段（320）と第2乱数発生手段（330）と第2暗号化キー照合手段（340）と前記第2暗号化キー照合手段（340）の照合結果に基づいて前記メモリデータの送受信の可否を決するデータ読出制限手段（350）とを備えたデータ記憶体である。これにより、データ記憶体の保持する（期日や金額等の）メモリデータを改竄すること等の不正使用が、ほぼ不可能となる。

【0026】〔第2の実施の形態〕本発明の第2の実施形態は、上述した解決手段および実施形態のデータ秘匿

装置が、他の複数装置とともに利用地域や利用日等の所定基準に従ってグループ分けされており、前記第1の秘匿解除データ及び前記第2の秘匿解除データの少なくとも一方は少なくとも一部が前記グループ分けに対応して設定されていることを特徴とする。これにより、異なるグループ間での不正流用を容易かつ確実に防止することができる。

【0027】例えば本発明のデータ秘匿装置が組み込まれたリーダライタ100（データ読取装置）及びデータキャリア200（データ記憶体）を自動改札装置およびリフト搭乗券として複数のスキー場に導入したような場合、各スキー場ごとに異ならせてキーK1（第1の秘匿解除データ）の値を設定するとともに、利用日ごとに異ならせてキーK2（第2の秘匿解除データ）の値を設定するとよい。こうすることで、新たな回路等を何ら付加しなくても、他のスキーのリフト券や前日のリフト券などについての改札誤りを避けることが可能となる。

#### 【0028】

【実施例】本発明のデータ秘匿装置を適用した一実施例としてのデータキャリアシステムについて、その具体的な構成を、図面を引用して説明する。図1は、その機能ブロック図であり、図2は、データアクセス装置としてのリーダライタ100の回路ブロック図およびフローチャートであり、図3は、データ記憶体としてのデータキャリア200の回路ブロック図である。

【0029】リーダライタ100は、マイクロプロセッサ14のプログラム処理が第1乱数発生手段120と第1暗号化キー照合手段130と第2暗号化キー返送手段140とを具現化するように変更されている点で、従来例におけるリーダライタ10と相違する。データキャリア200は、秘匿回路300が第1暗号化キー返送手段320と第2乱数発生手段330と第2暗号化キー照合手段340とを具現化するように秘匿回路30から拡張されている点で、従来例におけるデータキャリア20と相違する。なお、図1では、コイル11と伝送部13とを纏めて伝送部110とし、コイル21と制御回路230等とを纏めて伝送部210として示した。以下、重複する再度の説明は割愛し、これらの相違点を説明する。

【0030】リーダライタ100のマイクロプロセッサ14は、データキャリア200と通信可能になると、先ず、乱数R1（第1の乱数）を発生するようにプログラムされている（図2のステップS1を参照）。乱数発生は、一般的な疑似乱数を発生させるものでよく、シフトと加算とを繰り返しその度に一部を抽出して乱数とすること等で具体化され、乱数R1の値は毎回変化する。これにより、リーダライタ100は、第1の乱数R1を発生する第1乱数発生手段120を備えたものとなっている。さらに、マイクロプロセッサ14は、この乱数R1を伝送部13及びコイル11経由で交番電磁界として送出するようにもプログラムされている（ステップS

2)。これにより、乱数R1がデータキャリア200へ送信されるようになっている。

【0031】リーダライタ100のマイクロプロセッサ14は、その後、データキャリア200からの返信(C1)を待ってこれを受信する(ステップS3)。この返信(C1)はデータキャリア200によってキーK1

(第1の秘匿解除データ)が乱数R1で暗号化された暗号化キーC1(暗号化済み第1の秘匿解除データ)であることが期待されており、この暗号化キーC1に対して暗号化と逆の復号化処理が乱数R1を用いて施され、復号化した値F1を得る(ステップS4)。さらに、値F1がマイクロプロセッサ14付属のメモリに記憶済みのキーK1と同一値か否かを判別する(ステップS5)。これにより、リーダライタ100は、受信した暗号化キーC1について自己の保持するキーK1との照合を行う第1暗号化キー照合手段130を備えたものとなっている。

【0032】そして、比較結果が不一致のときにはその時点でそのデータキャリア200を対象とした通信を停止するが、比較結果が一致のときにはさらに以下の処理を続行する(ステップS5)。リーダライタ100のマイクロプロセッサ14は、引き続き、データキャリア200から乱数R2(第2の乱数)が送信されて来るのを待ってこれを受信すると(ステップS6)、この乱数R2を用いてキーK2(第2の秘匿解除データ)に暗号化処理を施して暗号化キーC2(暗号化済み第2の秘匿解除データ)を生成する(ステップS7)。この暗号化処理は掛け算あるいは排他的論理和などで具現化され、暗号化キーC2は、データキャリア200へ向けて送出され返送される(ステップS8)。これにより、リーダライタ100は、受信した乱数R2を用いてキーK2を暗号化しこの暗号化キーC2をデータキャリア200へ返送する第2暗号化キー返送手段140を備えたものとなっている。

【0033】そして、これらの一連の処理を終えてから、さらにデータキャリア200の準備が整うまでの所定時間が経過してから、本来のデータ読出等を開始するためにリードコマンドの送信を行う。しかも、上述したように暗号化キーC1とキーK1との比較結果が一致したときだけ、リードコマンドの送信を開始する。これにより、リーダライタ100は、第1暗号化キー照合手段130の照合結果に基づいてメモリデータの送受信の可否を決するデータ読出手段150を備えたものとなっている。

【0034】データキャリア200の秘匿回路300は、秘匿回路30に設けられていたシフトレジスタ31、32と比較回路33とカウンタ34と順序回路35とに加えて、受信データDIをシリアル入力としシフトクロックSKをタイミング信号とするシフトレジスタ301と、読出データDOをシリアル入力としシフトクロ

ックSKをタイミング信号とするシフトレジスタ302と、両シフトレジスタ301、302に保持されたデータに掛け算等の処理を施して暗号化する暗号化回路303とが設けられている。そして、リーダライタ100から乱数R1を受信すると、この乱数R1が受信データDIとしてシフトレジスタ301にロードされるとともにキーK1が読出データDOとしてシフトレジスタ302にロードされて、暗号化回路303によって暗号化キーC1が生成されるようになっている。また、制御回路230は、乱数R1の受信時にそのような制御を行うとともに暗号化キーC1をリーダライタ100へ返送するように制御回路23が改造されたものである。これにより、データキャリア200は、受信した乱数R1を用いてキーK1を暗号化しこの暗号化キーC1をリーダライタ100へ返送する第1暗号化キー返送手段320を備えたものとなっている。

【0035】また、秘匿回路300に、疑似乱数を算出することで発生ごとに値の変化する乱数R2を発生する乱数発生回路304が設けられるとともに、制御回路230に、暗号化キーC1の返送後これに続けて乱数R2をリーダライタ100へ送信するような制御シーケンスが付加されている。これにより、データキャリア200は、乱数R2を発生するとともにこれを暗号化キーC1の返送の後に送信する第2乱数発生手段330を備えたものとなっている。

【0036】さらに、秘匿回路300には、乱数R2を受けて保持するシフトレジスタ305と、シフトレジスタ32と比較回路33との間に介挿されシフトレジスタ32のキーK2をシフトレジスタ305の乱数R2で暗号化(F2)してから比較回路33へ送出する暗号化回路306とが設けられ、制御回路230は、乱数R2の送信後に暗号化キーC2を受信して初めて、これをシフトレジスタ31にロードさせ、比較回路33、カウンタ34、順序回路35を動作させるものである。これにより、データキャリア200は、受信した暗号化キーC2について自己の保持するキーK2との照合を行う第2暗号化キー照合手段340を備えたものとなっている。なお、順序回路35の出力を受けるANDゲート41の存在により、第2暗号化キー照合手段340の照合結果に基づいてメモリデータの送受信の可否を決するデータ読出制限手段350も備えたものとなっている。

【0037】このようなリーダライタ100及びデータキャリア200内に具現化されたデータ秘匿装置について、その使用態様及び動作を説明する。

【0038】かかるデータキャリアシステムでは、利用者が自己のデータキャリア200をリーダライタ100のコイル21に近づけてこれら一対のリーダライタ100及びデータキャリア200が交信可能な状態になると、まず、リーダライタ100が主導する秘匿解除データK1についての送受信および照合と、データキャリア

200が主導する秘匿解除データK2についての送受信および照合がおこなわれる。

【0039】秘匿解除データK1についての送受信および照合は、リーダライタ100の乱数発生手段120による乱数R1の発生およびその送信によって開始され、この乱数R1を受けたデータキャリア200の暗号化キー返送手段320による暗号化キーC1の返送で継続され、リーダライタ100の暗号化キー照合手段130による暗号化キーC1とキーK1との照合によって終了する。こうして、リーダライタ100からデータキャリア200へ乱数R1の通信伝文が送られるとともにデータキャリア200からリーダライタ100へ暗号化キーC1の通信伝文が送り返される（図1における二点鎖線を参照）。そして、乱数R1が毎回変化するので、暗号化キーC1も毎回変化し、キーK1は生の値が通信伝文に現れるということがない。

【0040】秘匿解除データK2についての送受信および照合は、データキャリア200の乱数発生手段330による乱数R2の発生およびその送信によって開始され、この乱数R2を受けたリーダライタ100の暗号化キー返送手段140による暗号化キーC2の返送で継続され、データキャリア200の暗号化キー照合手段340による暗号化キーC2とキーK2との照合によって終了する。こうして、データキャリア200からもリーダライタ100へ乱数R2の通信伝文が送られるとともにリーダライタ100からデータキャリア200へ暗号化キーC2の通信伝文が送り返される（図1の二点鎖線を参照）。そして、この場合も、乱数R2、暗号化キーC2が毎回変化するので、キーK2は生の値が通信伝文に現れるということがない。

【0041】そして、リーダライタ100においてキーK2の一致照合が成立し、さらにデータキャリア200においてもキーK1の一致照合が成立した場合だけ、メモリデータの送受信が行われる。すなわち、リーダライタ100がデータキャリア200へリードコマンドを送出し、これを受けてデータキャリア200がメモリ24から保持データを読み出してこれをリーダライタ100へ返送するなどの通信に基づく通常の処理が継続される（図1の二点鎖線を参照）。

【0042】こうして、リーダライタ100の主導する乱数R1及び暗号化キーC1の通信と、同じくリーダライタ100の主導するコマンド及びデータの通信との間に、それらとは逆にデータキャリア200の主導する乱数R2及び暗号化キーC2の通信が挿入されることで、メモリデータの送受信に先だつ秘匿解除データの送受信および照合が行われる。

【0043】

【発明の効果】以上の説明から明らかなように、本発明のデータ秘匿装置にあっては、傍受した通信の解読を困難にするため秘匿解除データを暗号化および複数化する

に際し、通信の主導側および応答側が入れ替わるようにしたことにより、一層確実に不正使用からメモリデータを保護することができたという有利な効果がある。

【図面の簡単な説明】

【図1】 本発明のデータ秘匿装置について、機能ブロック図である。

【図2】 そのデータ読取装置についての回路等ブロック図である。

【図3】 そのデータ記憶体についての回路ブロック図である。

【図4】 従来のデータ秘匿装置である。

【符号の説明】

- 10 リーダライタ（データ読取装置）
- 11 コイル（アンテナ；電磁誘導結合子）
- 13 伝送部
- 14 マイクロプロセッサ（MPU）
- 20 データキャリア（携帯形データ記憶体）
- 21 コイル（アンテナ；電磁誘導結合子）
- 22 整流回路（電源回路）
- 23 制御回路（制御部；伝送部）
- 24 メモリ
- 30 秘匿回路
- 31 シフトレジスタ（第1秘匿解除データ保持部）
- 32 シフトレジスタ（第2秘匿解除データ保持部）
- 33 比較回路（照合手段）
- 34 カウンタ
- 35 順序回路（判定部；データ読出制限手段）
- 41 ANDゲート（データ読出制限手段）
- 100 リーダライタ（データ読取装置）
- 110 伝送部
- 120 （第1）乱数発生手段
- 130 （第1）暗号化キー照合手段
- 140 （第2）暗号化キー返送手段
- 150 データ読出手段
- 200 データキャリア（携帯形データ記憶体）
- 210 伝送部
- 230 制御回路
- 300 秘匿回路
- 301 シフトレジスタ（受信乱数R1保持部）
- 302 シフトレジスタ（読出キーK1保持部；秘匿解除データ保持部）
- 303 暗号化回路（暗号化キーC1返送手段）
- 304 乱数発生回路（乱数R2発生手段）
- 305 シフトレジスタ（発生乱数R1保持部）
- 306 暗号化回路（暗号化キーC2照合手段）
- 320 （第1）暗号化キー返送手段
- 330 （第2）乱数発生手段
- 340 （第2）暗号化キー照合手段
- 350 データ読出制限手段
- CS チップセレクト

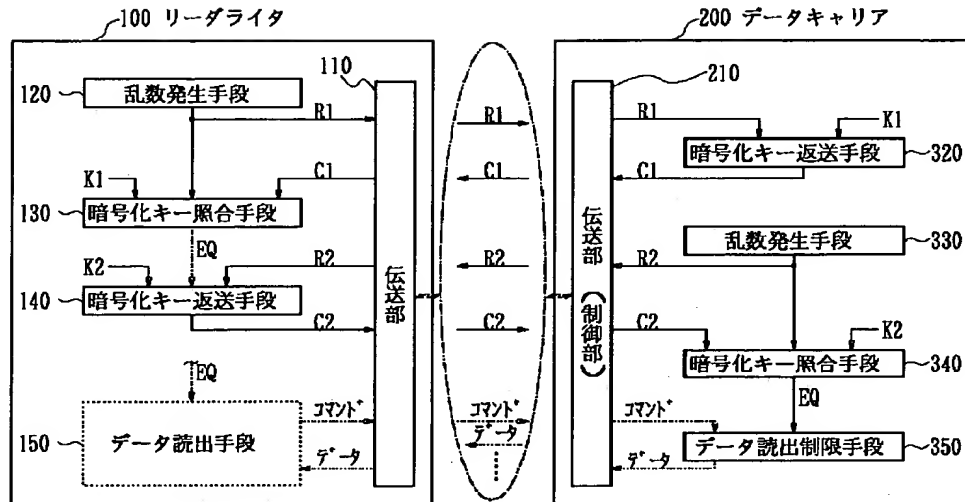


SK シフトクロック  
DI 受信データ  
DO 読出データ  
EQ 一致出力  
CNT カウント値

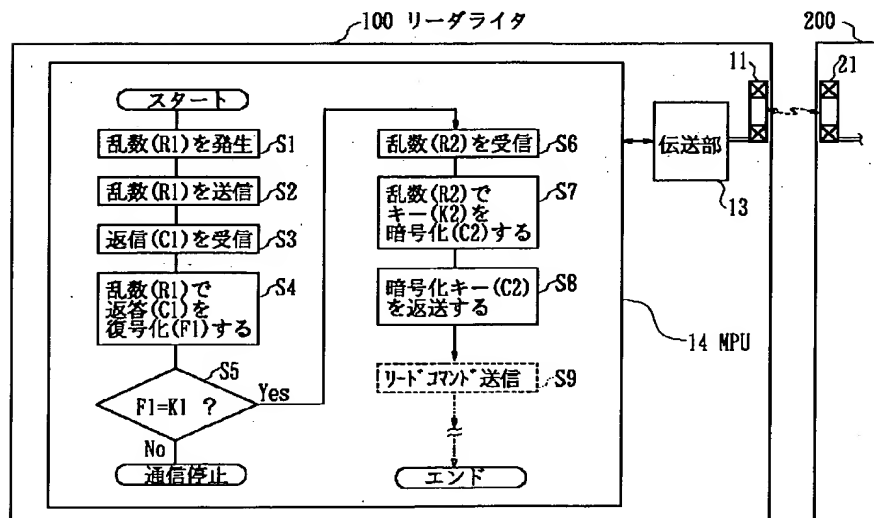
\* K1、K2 キー（秘匿解除データ）  
R1、R2 乱数（疑似乱数）  
C1、C2 暗号化キー（乱数で暗号化された秘匿解除データ）

\*

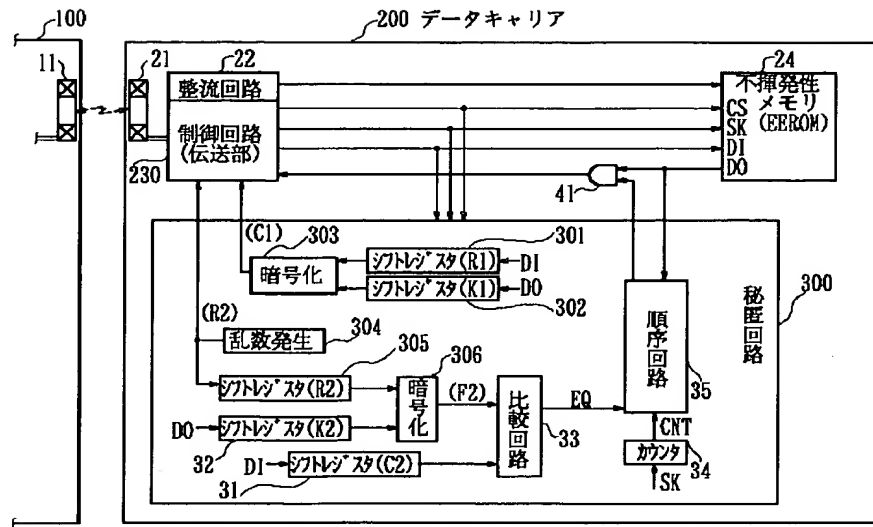
【図1】



【図2】



【図 3】



【図 4】

